



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/596,863

03/12/2007

Luis Ramos Robles

P18230-US1

1476

27045

7590

06/16/2009

ERICSSON INC.  
6300 LEGACY DRIVE  
M/S EVR 1-C-11  
PLANO, TX 75024

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

06/16/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



### **DETAILED ACTION**

The instant application having Application No. 10/596,863 is presented for examination by the examiner. Claims 30-32 and 46-49 have been amended and are pending.

### ***Response to Amendment***

#### ***Claim Objections***

Claims have been amended to overcome the previous claim objections.

Claims 46-49 are objected to because of the following informality: In claim 46, "the WLAN access server" should be "a WLAN access server". Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 112***

Claims have been amended to overcome the previous 112 rejections.

### ***Response to Arguments***

Applicant's arguments filed 5/13/09 have been fully considered but they are not persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., explaining the SSO mechanism and connecting SSO to HTTP) are not recited in

Art Unit: 2431

the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The prior art of Costa teaches the newly amended limitation of the independent claims as using an shared secret K and client identification information gained during an initial authentication process whereby the first service provider [SSO manager] lends the client's authentication validation to another service provider (0048-0050). The first service provider acts as the SSO manager because it provides SSO functionality to the user/client device. Also the authentication server 134 of Figure 1 acts to provide authentication information to service providers on behalf of the client device once said client device has authenticated with said authentication server. This allows the client device to take part in authentication protocols that it does not natively support (0034).

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 30-32, 46, 48, and 49 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2004/0225878 to Costa-Requena et al., hereinafter Costa.

As per claim 30, Costa teaches an apparatus arranged for receiving an access request in a telecommunication core network from a wireless local network-access server in a wireless local access network the access request sent by a user equipment of a user, the user being a subscriber of the telecommunication CN and being identified by a user's identifier included in the access request, the apparatus having a means for carrying out an authentication procedure with the UE through the WLAN-AS [RAS] in order to authenticate the user (0034);

and a means for computing at least one secret user's key (calculations are inherently performed on the Ki secret key employed by the GSM standard; 0029, 0052) usable as cryptographic material (0035 and 0048), the apparatus comprising:

a means for deriving from the cryptographic material a user's shared key (shared secret key; 0048) intended for SSO purposes (0050); and

a means for sending the user's shared key along with the user's identifier towards a SSO session manager serving a service network of a mobile network operator (0050).

As per claim 31, Costa teaches comprising means for being notified that a session [session layer] the access level of the WLAN-As has been established (0024-

Art Unit: 2431

0025), this notification triggering the sending of the user's shared key to a SSO session manager serving the MNO-SN (0036, 0045, 0050).

As per claim 32, Costa teaches means for being notified that a session at the access level of the WLAN-AS has been terminated, and means for forwarding this notification towards the session manager (0050) serving the service network in order to Inactivate a current master session for the user [single log-out].

As per claim 46, Costa teaches a user equipment usable by a user with a subscription in a telecommunication network, and arranged to access a telecommunication service network of a mobile network operator through a wireless local access network , the user equipment having means for carrying out an authentication procedure to authenticate the user with a core network (GSM; 0029), through the WLAN access server and

means for computing at least one secret user's key (calculations are inherently performed on the Ki secret key employed by the GSM standard; 0029, 0048 0052) usable as cryptographic material, the user's equipment comprising:

a means for deriving from the cryptographic material a user's shared key intended for SSO purposes (0035, 0048, and 0050);

a repository for storing the user's shared key (0035; SIM); and

a means for confirming to a session manager of the MNO-SN the user's shared key stored at the user's equipment (0048).

As per claim 48, Costa teaches a means for confirming to a session manager of the MNO-SN the user's shared key includes a means for processing the user's shared

Art Unit: 2431

key to obtain a key code [integrity check] to be transmitted to the session manager of the MNO-SN in the service network (0048).

As per claim 49, Costa teaches means for receiving an SSO cookie [security token] from the session manager of the MNO-SN, the SSO cookie to be included in all further service requests from the user's equipment as an SSO token (0034).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Costa in view of publication "Using GSM/UMTS for Single Sign-On" by Pashalidis and Mitchell hereinafter Mitchell.

As per claim 47, Costa is silent in disclosing means for confirming includes a means for downloading an SSO plug-in from an entity in the service network, the SSO plug-in running for confirming back the user's shared key. Mitchell's system of a single sign-on mechanism through a SIM based phone teaches that the protocol can be implement in a continuously running process (AKA 'service' or 'daemon') to minimized

Art Unit: 2431

the user's interaction (see page 141, last paragraph before section 4). The service running in the background would keep the user authenticated if the system requires him/her to ever re-authenticate. It would also allow the system to know that the user was still active in the network therefore not time-out the user. It would be beneficial to the Costa system to implement this feature because it would lessen the burden and interaction required by the user to stay authenticated in the network. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine this feature of Mitchell within the system of Costa to minimize the burden of the user to stay connected in the network.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of



Art Unit: 2431

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/596,863  
Art Unit: 2431

Page 9

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/  
Supervisory Patent Examiner, Art Unit 2431